dun & bradstreet

Dun & Bradstreet Austria GmbH

Technical and organizational measures for the protection of data

Version: October 2021

Table of contents

1. AREA OF APPLICATION

In accordance with the General Data Protection Regulation (GDPR), the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the varying likelihood and severity of risks for the rights and freedoms of natural persons. This document describes the measures which have been taken in order to comply with article 32 of the GDPR for the Austrian D&B company (hereinafter summarised as "D&B") namely by Dun & Bradstreet Austria GmbH, Jakov-Lind Straße 4/1, 1020 Vienna.

2. CONFIDENTIALITY MEASURES (ARTICLE 32 SECT 1 GDPR)

2.1. Entry control

Entry control serves to deny unauthorised parties access to technical facilities with which personal data is processed or used.
Access to the D&B offices is regulated by entry checks. For employees of D&B, they primarily consist of electronic keys which, to the extent of the access rights assigned to each key, allow entry to the offices.
Both the time (pertaining to use on certain days of the week and at certain times of day) as well as the place (certain parts of the place of business) of the access rights are adjusted according to the authorisations of the employee.
For external parties, the entry control is ensured by a central reception which records the data of the visitor. The visitor will be accompanied or supervised during their task by an employee of D&B at all times.
The IT systems of D&B are run on-site in the D&B offices. The data centres have been designed as a closed security area. Both constructional as well as technical entry protection is in place. The data centres are secured electronically and visitors may only gain access when accompanied by a D&B employee and are never left unsupervised. The required access logins are only issued upon prior application and under strict conditions. The use is logged.
Outside of business operating hours,the entrances and exits to the offices are monitored by video and alarm systems and both the premises as well as the critical interior areas of the building are additionally monitored by a security service.

2.2. Admission control

Admission control encompasses measures with which the use of data processing systems (logical security) by unauthorised parties is prevented.
Every D&B employee has his own personal login data for his computer to access the systems or data bases.
Work on D&B systems is only conducted by employees, which have signed a separate non-disclosure agreement and have been checked before hiring. The non-disclosure agreement contains an obligation to comply with data security as per § 6 of the Data Protection Amendment Act 2018. Should tasks take place via external logins, then these so-called VPN connections must be processed

with a state of the art encryption and an additional authentication. The identification with user name and safe password is obligatory.
The D&B IT systems are additionally protected against external interference by firewall technologies. The firewall is operated and maintained centrally by the parent company Bisnode AB, Solna (Sweden).

2.3. Access control

Access control includes measures which ensure that individuals, authorised to use a data handling system, can only access the data which is assigned to their access authorisation, and that personal data can not be read, copied, changed or deleted by unauthorised persons during processing or using and after saving.
D&B has defined and documented internal standards for the handling of authorisations. These are defined in the contract of employment or the employee handbook (secrecy, prohibition of transferring of passwords, etc.). New employees are trained accordingly in data handling.
The allocation of login details is a standardised process upon entering the company. The logins are given to the employee over the phone or in person, and the password and user name must be changed after the first login.
Passwords must be at least 8 characters long. They must contain both upper and lower case letters and numbers. The passwords must be changed every 60 days as per Windows Policy and the last 8 passwords can not be used repeatedly. If the password hasn't been changed in time, or the password has been falsely entered 5 times, then the user is automatically blocked. It is, of course, possible to change the current password at any time.
Every computer is set up with the automatic screen lock through the Windows Group Policy, which activates upon 10 minutes of non-use.
Access rights to files are maintained through the Windows Active Directory. Extended rights must be requested through a approval process via the relevant manager and in writing to the IT department.
Telework is conducted on computers provided by D&B. The connection to D&B is created via a centrally operated VPN tunnel.
Stationary laptops are secured with Kensington locks, mobile employee laptops have encrypted hard drives.
The access rights to file shares are determined by roles/ groups, where shares can be accessed by department (or function).
The details are regulated in the "Roles and Authorisation Concept" of D&B.
When an employee leaves the company, all logins to the system are immediately locked. All documents, issued keys and IT devices are redeemed.
Old data carriers and security tapes are physically destroyed.
All users in the active directory and their rights in the network are regularly checked and changed and adapted, if needed.

2.4. Separation control

The separation regulation includes measures which ensure that data, which has been logged for different purposes, can be processed separately.
With regard to the general processing of their data at D&B (employee data, supplier data, customer master data), the separation regulation has been implemented for example by physically separating and saving to separate systems or data carriers, separation of the production, test and development

environment of our applications and IT systems, relevant authorisation concepts as well as data base rights. Furthermore, a software-based logical client separation has also been implemented.
Within the scope of data processing by D&B for business purposes and for receipt and provision of the data of their customers within the scope of the information transaction at D&B in particular, a separation, as laid down by data protection, takes place predominantly on the basis of the application. All supplied data packages are processed strictly separately so that a possible overlapping of customer data is excluded. All required (hardware and software) arrangements have been made.

3. INTEGRITY MEASURES (ARTICLE 32 SECT 1 GDPR)

3.1. Transfer control

Transfer control includes measures which ensure that personal data can not be read, copied, changed or deleted by unauthorised persons during electronic transfer, transport or saving to data carriers, and that it is possible to check and determine at which point a transfer of personal data through data transmission devices is intended.
With regard to the general processing of their data at D&B (employee data, supplier data, customer master data), transfer control (transmission control, transport control, communication control) is accordingly ensured through appropriate technical measures.
Only transmission methods which allow an encryption of data (SFTP, VPN tunnel, encryption with PGP) are used to transfer data to / from customers.
D&B systems are isolated from other systems by a firewall cluster and an IPS system (intrusion prevention) is in place for early detection / prevention of attempted break-ins.
Backups which are given to an external IT security company, within the scope of the weekly back-up cycle, are encrypted and are delivered in a closed container.
Within the scope of data processing by D&B for business purposes and for receipt and provision of the data of their customers within the scope of the information transaction at D&B in particular, the transfer control is ensured through logging of all data processing steps. Data that has been defined as particularly classified is, in agreement with the controller, additionally encrypted when transferred via public networks. The data of their customers, which D&B processes on behalf of the customer, are only given to third parties upon written authorisation by the customer, as per the legal regulations for contract data processing (§ 28 GDPR).

3.2. Input control

Input control includes measures which ensure that it is possible to retrospectively check and determine whether and by whom personal data has been entered into, changed or deleted from the data processing system.
The data can only be entered by employees that have access to the data.
Access to research data is only enabled during processing procedures. Which employee processed the data at what time is logged.
Furthermore, automatic logs of "certain actions" of processes are created on the systems. The logs of the "certain actions" relate to processes which serve to maintain the system operation, billing procedures and to fulfil legal storage requirements.

4. AVAILABILITY AND CAPACITY MEASURES (ARTICLE 32 SECT 1 GDPR)

4.1. Availability control

Availability control includes measures which ensure that personal data is protected against accidental destruction or loss.
D&B operates numerous delivery systems with uninterruptible power supply.
Furthermore, central systems are also replicated in a secondary computer centre to ensure availability for quick disaster recovery. The procedure is documented in the disaster recovery plan.
D&B systems are isolated from other systems by a firewall cluster and an Intrusion Prevention System is in place for early detection / prevention of attempted break-ins.
Furthermore, the system programmes and hardware are regularly updated to state of the art standard. A central anti-virus system and email spam filters are also in operation.
Furthermore, data availability, in particular securing against data loss through technical failure or accidental deletion, is ensured through regular data securing and backups of the entire system and data, which are filed weekly with an external IT security company.
Furthermore, a monitoring tool is in place which continually checks the D&B server and applications and raises an alarm, if necessary, enabling early problem resolution.
The computer centre is structurally separate and only accessible with keys. A large air-conditioning system cools the systems in the room. Smoke detectors as well as temperature and water ingress sensors are in operation.
Personal data is saved by D&B for the length of time which is required to complete the service. It is then deleted, unless a further saving of data is required for additional purposes to adhere to commercial and tax-related storage regulations or to maintain evidence within the scope of the statute of limitations.

5. MEASURES FOR REGULAR CHECKS, ASSESSMENTS AND EVALUATIONS (ARTICLE 25 SECT 1 GDPR)

5.1. Data protection management

Data protection management defines the internal measures for the unique requirements of data protection.

	Measures
01	D&B employs an occupational data protection officer.
02	D&B has an IT- / Information security officer.
03	Deputy regulations for the DP officer are in place at D&B (responsible for the IT-infrastructure used by the contractor).
04	The officers for IT / Information security and data protection at D&B are appropriately trained and have an appropriate level of technical knowledge and an appropriate personal aptitude.
05	The officer for IT- / Information security and data protection of the contractor are appropriately integrated in the organisation structure (as a specialist team to management or a similar independent position).

06	Regular basic trainings for employees for information security and data protection are held.
07	Processes are in place for regular evaluation and update of the available trainings to the required level and to changes to the requirements of frame agreements (changes to the laws, new laws and regulations).
08	The employees, which deal with personal data, are instructed in and obligated to adhere to data protection and the appropriate handling.
09	A primary regulation / policy for data protection is in place.
10	A primary regulation / policy for IT security is in place.
11	These regulations are centrally filed and are available to all employees.
12	The provisions resulting from these regulations are to be observed in work procedures, or similar.
13	Documented processes for identification, analysis, evaluation and consideration of changes to the requirements (e.g. data protection laws) as well as the IT procedures and processes (data protection impact assessment, new applications, new IT systems, etc.) are in place.
14	Documented processes for identification, analysis, evaluation of data protection issues in relation to changes as well as the conception of appropriate measures to prevent repeated unauthorised access (connection of change management to incident management) are in place.

5.2. Incident response management

D&B is aware of the legal communication obligations and has sensitised and trained their employees to recognise potential notifiable violations. An appropriate communication process has been defined. The addressees of the communication (customer services) and the employees are aware whom they must approach in case of a data protection violation. Furthermore, a procedure for immediate processing, following receipt of the communication, has also been implemented. The members of the "crisis team" have been defined and the evaluation of the issue as well as potential triggering of the response is ensured.
The Incident Response Management for data protection violations is associated with IT-Incident Management, Security Incident Management, Emergency or Crisis Management of Bisnode AB.

5.3. Data-protection-friendly default settings

For the implementation of art 24 sect 2 GDPR, D&B has created a „Group Privacy by Design & Default Guideline". This stipulates, that D&B must proactively and not reactively integrate data protection into all areas and already consider data protectionin the design phase of offers. For D&B, privacy by design compliance is not merely a question of user experience. Appropriate technical and safety-related measures to protect the user data and personal data are pursuant to an appropriate level of compliance.
Furthermore, D&B has prepared a „Group Retention Policy". This is a template document, which is implemented with local discrepancies for every market. To that end, D&B has implemented an appropriate deletion concept for personal data in Austria.

5.4. Project control

Project control includes measures which ensure that personal data, which is being processed been on behalf of a controller, is only processed according to the instructions of the controller.
Whenever processing personal data on behalf of a controller, D&B will always conclude a written contract for processing data on behalf of a controller which must include legally required content as per § 28 sect 9 GDPR. D&B also provides its own contract templates, which the controller can use for the ommission.
Contractual obligations regulate that D&B can only process the data of the controller on instruction of the latter, ensuring the confidentiality of the data and, provided the controller does not stipulate otherwise, no copies of customer data are saved to the general D&B company database.
Furthermore, descriptions of the technical and organisational security measures at D&B are part of every contract for the processing of data on behalf of a controller with D&B, in that this document shall be added as an appendix to said contract.

Dun & Bradstreet Austria GmbH
October 2021